

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listing of claims in the above-referenced application.

Listing of Claims:

1. (Previously Presented) A computer implemented method of scanning a storage device for viruses, comprising:

determining physical portions of the storage device that have been modified since a previous virus scan using information about the physical portions without using information about a file structure, a file system, or a file type;

detecting, by the storage device, write operations to tracks of the storage device;

providing, to an antivirus unit by the storage device, information indicating which tracks of the storage device have been accessed for a write operation; and

scanning, by the antivirus unit, at least parts of the physical portions for viruses, wherein scanning is performed without using information about a file structure, a file system, or a file type, and wherein scanning is performed on those tracks to which write operations have been directed in accordance with the information provided by the storage device.

2. (Original) A method, according to claim 1, wherein the physical portions correspond to tracks of the storage device.

3. (Original) A method, according to claim 1, wherein the physical portions correspond to sectors of the storage device.

4. (Original) A method, according to claim 1, wherein the physical portions correspond to subportions of the storage device.

5. (Original) A method, according to claim 1, wherein determining the physical portions of the storage device that have been modified includes:

creating a table that is indexed according to each of the portions and has entries indicating whether a corresponding one of the portions has been modified, the entries being cleared after a virus scan to indicate that no portions have been modified; and

setting a specific one of the entries in response to a corresponding one of the portions of the storage device being subject to a write operation.

6. (Original) A method, according to claim 5, wherein creating the table includes copying an other table provided by the storage device.

7. (Original) A method, according to claim 5, wherein creating the table includes using an other table provided by the storage device.

8. - 21. (Cancelled)

22. (Previously Presented) A computer program product for scanning a storage device for viruses, the computer program product including a computer-readable medium with executable code stored thereon for:

determining physical portions of the storage device that have been modified since a previous virus scan using information about the physical portions without using information about a file structure, a file system, or a file type;

detecting, by the storage device, write operations to tracks of the storage device;

providing, to an antivirus unit by the storage device, information indicating which tracks of the storage device have been accessed for a write operation; and

scanning, by the antivirus unit, at least parts of the physical portions for viruses, wherein the scanning is performed without using information about a file structure, a file system, or a file type, and wherein scanning is performed on those tracks to which write operations have been directed in accordance with the information provided by the storage device.

23. (Original) A computer program product, according to claim 22, wherein the physical portions correspond to tracks of the storage device.

24. (Original) A computer program product, according to claim 22, wherein the physical portions correspond to sectors of the storage device.

25. (Original) A computer program product according to claim 22, wherein the physical portions correspond to subportions of the storage device.

26. (Previously Presented) A computer program product, according to claim 22, wherein said code for determining the physical portions of the storage device that have been modified includes code for:

creating a table that is indexed according to each of the portions and has entries indicating whether a corresponding one of the portions has been modified, the entries being cleared after a virus scan to indicate that no portions have been modified; and

setting a specific one of the entries in response to a corresponding one of the portions of the storage device being subject to a write operation.

27. (Previously Presented) A computer program product, according to claim 26, wherein said code for creating the table includes code for copying an other table provided by the storage device.

28. (Previously Presented) A computer program product, according to claim 26, wherein said code for creating the table includes code for using an other table provided by the storage device.

29. - 40. (Cancelled)

41. (Previously Presented) An antivirus unit, comprising:

- means for coupling to at least one storage device;
- means for determining physical portions of the storage device that have been modified since a previous virus scan using information about the physical portions without using information about a file structure, a file system, or a file type;
- means for receiving, from the at least one storage device, information determined by the at least one storage device indicating which tracks of the at least one storage device have been accessed for a write operation; and
- means for scanning at least parts of the physical portions for viruses, wherein scanning is performed without using information about a file structure, a file system, or a file type, and wherein scanning is performed on those tracks to which write operations have been directed in accordance with the information provided by the storage device.

42. (Original) An antivirus unit, according to claim 41, wherein the physical portions correspond to tracks of the storage device.

43. (Original) An antivirus unit, according to claim 41, wherein the physical portions correspond to sectors of the storage device.

44. (Original) An antivirus unit, according to claim 41, wherein the physical portions correspond to subportions of the storage device.

45. (Original) An antivirus unit, according to claim 41, further comprising:
a table that is indexed according to each of the portions and has entries indicating whether a corresponding one of the portions has been modified, the entries being cleared after a virus scan to indicate that no portions have been modified; and
means for setting a specific one of the entries in response to a corresponding one of the portions of the storage device being subject to a write operation.

46. (Original) An antivirus scanning unit, according to claim 41, wherein said means for coupling includes means for coupling to only one storage device.

47. (Original) An antivirus unit, according to claim 41, wherein said means for coupling includes means for coupling to more than one storage device.

48. (Original) An antivirus unit, according to claim 41, further comprising:
means for coupling to at least one host.

49. (Original) An antivirus unit, according to claim 48, wherein said antivirus unit is interposed between said at least one storage device and said at least one host.

50. (Original) An antivirus unit, according to claim 48, wherein said antivirus unit is implemented as a process running on the at least one host.

51. (Original) An antivirus unit, according to claim 41, wherein said antivirus unit is implemented using stand alone hardware.

52. (Original) An antivirus unit, according to claim 41, wherein at least a portion of the antivirus unit is provided on at least some controllers for the at least one storage device.

53. - 62. (Cancelled)

63. (Previously Presented) The method of Claim 1, wherein said storage device includes one or more sectors, and the method further comprising:

determining, for each sector of said storage device for a current virus scan, whether said each sector has been modified since a previous scan; and

for said current virus scan, scanning only those sectors determined to have been modified since said previous scan.

64. (Previously Presented) The computer program product of Claim 22, wherein said storage device includes one or more sectors, and the computer-readable medium further comprising code stored thereon for:

determining, for each sector of said storage device for a current virus scan, whether said each sector has been modified since a previous scan; and

scanning only those sectors determined to have been modified since said previous scan.

65. (Previously Presented) The antivirus unit of Claim 41, wherein said storage device includes one or more sectors, and the antivirus unit further comprising:

means for determining, for each sector of said storage device for a current virus scan, whether said each sector has been modified since a previous scan; and

means for scanning only those sectors determined to have been modified since said previous scan.

66. (New) The method of Claim 1, wherein the antivirus unit is included in the storage device.

67. (New) The method of Claim 66, wherein the antivirus unit is included in a disk controller of the storage device.

68. (New) The method of Claim 67, wherein the antivirus unit is included as software running on the disk controller.

69. (New) The method of Claim 67, wherein the antivirus unit is configured to use at least a portion of hardware that is separate from hardware of the disk controller.

70. (New) The method of Claim 67, wherein the disk controller is a first disk controller of a plurality of disk controllers included in the storage device, the antivirus unit is a first antivirus unit of a plurality of antivirus units included in the storage device, and each of said plurality of disk controllers includes a different one of said plurality of antivirus units.

71. (New) The antivirus unit of Claim 41, wherein said antivirus unit accessess data on the at least one storage device over a first connection and the information is provided on a second connection different from the first connection between said antivirus unit and the at least one storage device.